FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1353814-000

Total Deleted Page(s) = 1
Page 21 ~ b1; b3; b6; b7C; b7E;

XXXXXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X For this Page X
XXXXXXXXXXXXXXXXXXXXXXX

b1 b3 b7E b6 b7C

~~SECRET//ORCON/NOFORN~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 08/17/2016

To: Washington Field

From: Washington Field
CI-13
Contact: IA

Approved By:

Drafted By:

b3 b6 b7C b7E

(U) **Case ID #:** (X) -CYBER - 40

(U) **Title:** (X) MIDYEAR EXAM;
MISHANDLING OF CLASSIFIED;
UNKNOWN SUBJECT OR COUNTRY;
SENSITIVE INVESTIGATIVE MATTER (SIM)

Synopsis: (U//~~FOUO~~) Provides a summary of findings for all computer intrusion analysis conducted in captioned investigation.

b6 b7C

Classified By:
Derived From: FBI NSIC dated 20130301
Declassify On: 20411231

(X) b1 b3 b7E

~~SECRET//ORCON/NOFORN~~ (X)

this agent serial 40

b1 b3 b7E

[redacted] (S)

b1
b3
b7E

(U) **Details:** (S//~~NF~~) The purpose of this communication is to provide a summary of findings for all computer intrusion analysis conducted in support of captioned investigation. The analysis related to each of the events described below has been serialized in greater detail in MIDYEAR EXAM, Cyber sub-file.

(U//~~FOUO~~) This communication is split into two parts: general cyber analysis conducted over the course of the investigation; and cyber-related events that warranted further analysis, each of which is summarized individually.

(U) GENERAL CYBER INTRUSION ANALYSIS

(U//~~FOUO~~) INTRUSION ANALYSIS OF E-MAIL SERVERS AND DEVICES

(U//~~FOUO~~) FBI Operational Technology Division's Investigative Analysis Unit (IAU) conducted forensic analysis of images of the BRYAN PAGLIANO server[a] and the PLATTE RIVER NETWORK (PRN) server, to include media from DATTO backups and supplemental PRN files [redacted]

[redacted]

b6
b7C
b7E

[a] (U//~~FOUO~~) The oldest Windows Security Event logs available to the FBI from the PAGLIANO Server were from June 2013. As such, analysis of login data for accounts hosted on the server—to include CLINTON's—was limited.

b1
b3
b7E

[redacted]

b6
b7C
b7E

(U//~~FOUO~~) For IAU's complete report and details of the event related to [redacted] see [redacted]-CYBER, serials 17 and 37, respectively.

b3
b6
b7C
b7E

(U//~~FOUO~~) ANALYSIS OF DEVICES USED TO CULL CLINTON'S WORK E-MAILS

[redacted]

b3
b7E

(U) SIGNATURE DEVELOPMENT

(U) (~~S~~//~~NF~~) In support of captioned investigation,

[redacted]

b7E

through computer intrusion methods, [ ] b7E

[ ]

~~(S//NF)~~ Select U.S. Government (USG) agencies were furnished [ ]

[ ]

Division. The Executive Office of the President and DoS's Information Resource Bureau were unable to search the requested fields. [ ] b1 b3 b7E

[ ]

[ ] b7E

(U//~~FOUO~~) For more detailed information related to efforts concerning [ ] see [ ] CYBER, serial 9. b3 b7E

(U) IP ADDRESS ANALYSIS

(U) (S//~~NF~~) In support of captioned investigation, writers identified a total of [ ] b7E

[ ]

(U) (S//~~NF~~) Research and analysis focused heavily on the

b1 b3 b7E

remaining [redacted] IP addresses, which resolved to USG entities: the Executive Office of the President (EOP), U.S. Department of State, and U.S. Senate. Findings on [redacted] of the IP addresses are detailed at length in MIDYEAR EXAM, Cyber sub-file, serial 19. Of note, however, are the results found for IP address [redacted]

b7E

[redacted]

b1 b3 b7E

(U) E-MAIL ADDRESS ANALYSIS

(S//~~NF~~) Queries on [redacted] e-mail addresses associated with individuals CLINTON regularly communicated with yielded positive hits in various FBI databases. [redacted] Other results [redacted]

b1 b3 b7E

[redacted]

b1 b3 b7E

highlighted attempts by criminal actors to log in to an ICLOUD account for HDR22@CLINTONEMAIL.COM, which was used by CLINTON. Details about the various spear-phishing attempts and the illegitimate ICLOUD login attempts can be found in [redacted] CYBER, serials 7 and 15.

(S//~~NF~~) A review of approximately [redacted] e-mail addresses found in confirmed classified e-mail exchanges CLINTON was a part of was also conducted. The accounts were queried in [redacted] and

[redacted]

(U//~~FOUO~~) Complete details about the review of the [redacted] accounts can be found in [redacted] CYBER, serial 8.

(U) DOMAIN NAME ANALYSIS

[redacted]

b1
b3
b7E

[redacted]

b1
b3
b6
b7C
b7E

(U) DEVICE IDENTIFIERS ANALYSIS

(~~S~~//~~NF~~) FBI database checks were conducted on approximately [redacted] electronic device identifiers ranging from [redacted] and serial IDs associated with handheld devices associated with CLINTON. The unique values were queried and [redacted] returned negative hits. [redacted] No additional research was conducted on [redacted] given that their associated case files are [redacted] in Sentinel.

b1
b3
b7E

(U//~~FOUO~~) Full details of the device queries conducted can be found in [redacted]-CYBER, serial 25.

b3
b7E

(U//~~FOUO~~) CLINTON ACCOUNT LOGINS TO THE PAGLIANO SERVER

(U//~~FOUO~~) Logins for CLINTON's e-mail accounts spanning from 04/18/2009 to 06/30/2013 were analyzed to determine when CLINTON may have begun using the PAGLIANO Server; possible suspicious login activity while her account was hosted on the PAGLIANO Server; and whether logins were conducted from high-threat countries CLINTON traveled to during her tenure as U.S. Secretary of State.

(U//~~FOUO~~) Analysis was unable to determine the exact date of when HDR22@CLINTONEMAIL.COM was first hosted on the PAGLIANO Server. However, available IIS log data revealed logins between 04/18/2009 and 06/30/2013 were conducted from [redacted] unique IP addresses, [redacted] of which resolved to the United States and [redacted] to foreign countries.

b7E

(U//~~FOUO~~) The majority of US-based IP addresses resolved

[redacted]

b1
b3
b7E

b1
b3
b7E

to public ISPs, and [redacted] to USG entities—[redacted] to DoS and [redacted] to the U.S. Air Force (USAF). Use of the [redacted] USG IP addresses stood out, as CLINTON is known to not have had a computer terminal while at DoS, and repeated logins in 2011 and 2012 from IP addresses resolving to [redacted] seemed unusual. b7E

(U//~~FOUO~~) Statements provided to the FBI throughout the course of captioned investigation noted a limited number of individuals had authorized access to CLINTON's e-mail account, leading to the conclusion that logins conducted from DoS IP addresses were likely carried out by CLINTON's aides.

(U//~~FOUO~~) Regarding logins originating from the [redacted] USAF IP addresses, it is unclear why CLINTON's account would have connected to the PAGLIANO Server using USAF infrastructure. A possible explanation, however, is that CLINTON's iPad devices perhaps connected to the wireless network aboard the C-32 airplane she traveled on when on official business, which was a USAF-operated aircraft. This is a likely explanation, as the dates of activity reflected on the IIS logs correlated with CLINTON's official overseas travel schedule, as published by DoS. b7E

(U//~~FOUO~~) Logins conducted from overseas locations also correlated with CLINTON's official travel schedule, except for logins from [redacted]. Analysis of the related [redacted]--and knowing that CLINTON aides had authorized access to her e-mail account--make it likely that logins from [redacted] were carried out by CLINTON staff members, though this could not be confirmed. b7E

(U//~~FOUO~~) Additional details related to login analysis conducted for CLINTON's accounts can be found in [redacted]-CYBER, serial 38. b3 b7E

(U//~~FOUO~~) ANALYSIS OF SECNAP ALERTS & [redacted] EVENTS b7E

(U//~~FOUO~~) In the months following CLINTON's departure from DoS, her personal e-mail server's content was migrated to a server administered by PLATTE RIVER NETWORKS (PRN), who contracted with SECNAP NETWORK SECURITY CORPORATIONS to set up an intrusion detection and intrusion prevention (IDS/IPS) solution called CLOUDJACKET. The IDS/IPS sent alert e-mails when potentially malicious activity was directed at the server administered by PRN. Analysis of the e-mail messages between July 2013 and October 2015 found that [redacted] b7E

[redacted]

b1
b3
b7E

b1
b3
b7E

[redacted]

b7E

(U//~~FOUO~~) Analysis of activity captured by one of the firewalls installed on the PRN Server revealed that [redacted]

b7E

[redacted] Further inspection of the events found that [redacted]

Subpoenas were issued for [redacted] A determination was made not to interview [redacted]

(U//~~FOUO~~) Additional details related to the analysis conducted above can be found in [redacted]-CYBER, serials 27 and 30.

b3
b7E

(U) ANALYSIS OF SPECIFIC CYBER-RELATED EVENTS

[redacted]

b1
b3
b6
b7C
b7E

[redacted]

b7A
b7E

b1
b3
b7E

b1
b3
b7E

FEDERAL BUREAU OF INVESTIGATION

b1
b3
b6
b7C
b7E

(U//~~FOUO~~) COMPROMISED PERSONAL E-MAIL ACCOUNTS (2011)

b1
b3
b7E

(U//~~FOUO~~) [redacted]

b1
b3
b6
b7C

[redacted] X

(X//~~NF~~) [redacted] obtained for the aforementioned account identified JACOB SULLIVAN (SULLIVAN), CLINTON's former Deputy Chief of Staff at DoS, as the subscriber. [redacted]

[redacted] X

b1
b3
b6
b7C
b7E

(X//~~NF~~) For more detailed information related to SULLIVAN's account compromise, see [redacted]-CYBER, serial 3.

b3
b6
b7C
b7E

(U//~~FOUO~~) [redacted]

b1
b3
b7E

[redacted]

b1
b3
b6
b7C
b7E

(U) (~~S~~//~~NF~~) For more detailed information related to [redacted] account compromise, see [redacted]-CYBER, serial 4.

b3
b6
b7C
b7E

(U//~~FOUO~~) COMPROMISE OF SIDNEY BLUMENTHAL'S PERSONAL E-MAIL ACCOUNT (2013)

(U//~~FOUO~~) On or about 03/14/2013, SIDNEY BLUMENTHAL's (BLUMENTHAL) personal American Online (AOL) account was compromised by MARCEL LEHEL LAZAR (LAZAR), aka GUCCIFER, a Romanian hacker. BLUMENTHAL, a former political aide to President WILLIAM J. CLINTON and unofficial advisor to CLINTON during her tenure as U.S. Secretary of State, authored and sent CLINTON numerous e-mails and memorandums covering a wide range of foreign policy and intelligence matters. Over the course of CLINTON's tenure, BLUMENTHAL sent [redacted] e-mails, [redacted] of which contained information[h] deemed classified after classification review.

b7E

(U//~~FOUO~~) Following BLUMENTHAL's account compromise, LAZAR distributed a screenshot listing the filename of 19 unique memos pilfered from the victim's account to 31 news media outlets, some of them foreign. Review of the filenames revealed [redacted]

b7E

[redacted]

It is unknown if--in addition to the screenshot mentioned

[h] (U //~~FOUO~~) Classification review of documents authored and sent by BLUMENTHAL determined [redacted] memos are currently classified ~~CONFIDENTIAL~~ and [redacted] classified ~~SECRET~~.

b7E

b6
b7C

above--LAZAR also distributed soft copies of the memos to reporters.

(U//~~FOUO~~) ALLEGED COMPROMISE OF CLINTON'S E-MAIL SERVER

(U//~~FOUO~~) Shortly after being extradited to the United States on 03/31/2016 to face criminal charges, LAZAR revealed to FOX NEWS that he had compromised CLINTON's personal e-mail server. [redacted] b7E analysis of the approximate dates of when LAZAR claimed he hacked the CLINTON server did not reveal direct evidence of a compromise, though [redacted] foreign IP addresses[1] were captured in IIS logs in the week following BLUMENTHAL's account compromise. There was insufficient data to determine whether LAZAR may have been behind the activity associated with the [redacted] IP addresses in question, or whether the activity may have been conducted by individuals with whom LAZAR shared the BLUMENTHAL memos. When interviewed by the FBI on 05/26/2016, LAZAR stated he lied to FOX NEWS about hacking in to CLINTON's server.

(U//~~FOUO~~) For complete details related to BLUMENTHAL's account compromise; memos he sent to CLINTON; LAZAR's claims to FOX NEWS; and follow-up analysis conducted by writers, see [redacted]-CYBER, serials 6, 29, 31, 32, 35, and 39. b3 b7E

(U//~~FOUO~~) ATTEMPTED COMPROMISE OF ICLOUD ACCOUNT (2015)

(U//~~FOUO~~) Analysis was conducted on [redacted] login attempts to the APPLE ICLOUD account associated with the e-mail address HDR22@CLINTONEMAIL.COM. [redacted] revealed the activity occurred between 03/03/2015 and 12/13/2015, with [redacted] attempts made [redacted] b7E

(U//~~FOUO~~) The following table depicts: [redacted] b7E

[redacted]

[redacted] b7E

[1] (U) [redacted] b1 b3 b7E

b1
b3
b7E

b7E

(U//~~FOUO~~) Logical investigative follow-up was conducted on each of the above IP addresses, with certain results worth highlighting in this document.

(U//~~FOUO~~)

b4
b7E

(U//~~FOUO~~) The subscriber of IP addresses was determined to be to company located in A total of login attempts were conducted from IP addresses from 03/03/2015 to 03/06/2015, all during normal business hours.

(U//~~FOUO~~) Chief Executive Officer of confirmed aforementioned IP addresses were assigned to the company as of late March 2016, and may have belonged to in the past. IP address was dedicated to the company's which described as utilized that IP address to conduct

b4
b6
b7C
b7E

(U//~~FOUO~~) does not maintain historical logs for searches that are conducted by their clients.

b4
b6
b7C
b7E

b1
b3
b7E

b1
b3
b7E

[redacted]

b4
b7E

(U//~~FOUO~~) At this time, no additional information has been identified to explain the [redacted] login attempts to the HDR22@CLINTONEMAIL.COM ICLOUD account. Of significance is that the [redacted] login attempts began on 03/03/2015, which occurred a day after THE NEW YORK TIMES' (NYT) release of an article noting CLINTON's use of a personal e-mail system for official business.

b7E

(U//~~FOUO~~) Full details of [redacted] interview can be found in [redacted] CYBER, serial 16.

b3
b6
b7C
b7E

(U//~~FOUO~~) [redacted]

(U//~~FOUO~~) Another significant finding related to login attempts to the ICLOUD account associated with HDR22@CLINTONEMAIL.COM involved statements made by [redacted] the subject of FBI investigation [redacted] admitted that he attempted to access many celebrities' ICLOUD accounts, including the one associated with HDR22@CLINTONEMAIL.COM. [redacted] provided that his activities were primarily conducted from [redacted] and he denied gaining access to the account of interest. As he recalled, during his attempts to access the account he was [redacted] which led [redacted] to assess the account was an older one and likely had little information of value in it.

b6
b7A
b7C
b7E

(U//~~FOUO~~) Investigation in this matter determined that [redacted] likely was responsible for [redacted] logon attempts to the HDR22@CLINTONEMAIL.COM ICLOUD account. Those attempts originated from [redacted] admitted attempting to log in to ICLOUD accounts from [redacted] was identified in the San Francisco investigation as being [redacted] Lastly, given that [redacted] admitted to conducting unauthorized login attempts to ICLOUD accounts [redacted] were obtained. Review of these led writers

b6
b7C
b7E

b1
b3
b7E

to assess that possibly was responsible for the login attempt No additional evidence, however, was identified to corroborate

(U//~~FOUO~~) Full details of failed APPLE ICLOUD attempts can be found in -CYBER, serial 7.

(U//~~FOUO~~) ATTEMPTED LOGINS TO EXCHANGE SERVER AND DOMAIN CONTROLLER (2015)

(U//~~FOUO~~) This investigation determined that on 03/02/2015 the NYT published an article documenting CLINTON's use of a private e-mail server[j] and her personal e-mail address of HDR22@CLINTONEMAIL.COM. The public release of that information led to an increase in firewall activity and failed login attempts to the Microsoft Exchange server and domain controller associated with the domain.

(U) IIS LOG ANALYSIS

(U//~~FOUO~~) Analysis of the IIS logs subsequent to 03/02/2015 was conducted and a review of the most frequent user accounts that did not successfully authenticate to the Exchange server was conducted. The user accounts were most frequently used for failed login attempts. This activity was expected, as the targeting of known or suspected user accounts is consistent with that of malicious cyber actors.

(U//~~FOUO~~) Failed login attempts with usernames, including the handle, could be attributed to attackers who gleaned the account information from the NYT article. However, the failed login attempts during this timeframe could also be attributed to that of a legitimate user who accidentally entered an invalid password. More indicative of potential cyber attackers, nonetheless, are the failed login attempts that occurred with the usernames of

[j] (U//~~FOUO~~) For most of CLINTON's tenure as U.S. Secretary of State, her e-mail traffic was hosted on a private e-mail server administered by BRYAN PAGLIANO, content of which was migrated to a new server administered by PLATTE RIVER NETWORKS beginning the summer of 2013.

b1 b3 b7E

[redacted] b7E

(U) DOMAIN CONTROLLER FIREWALL LOGS

(U//~~FOUO~~) Firewall logs obtained from the domain controller associated with CLINTONEMAIL.COM were reviewed. The review identified that subsequent to 03/02/2015, several unauthorized access attempts from US-based and foreign IP addresses were captured by the firewall, specifically between 03/03/2015 and 03/05/2015. The domain controller captured unauthorized login attempts using several invalid login names. Given the publicity of the CLINTONEMAIL.COM domain, this type of behavior on the domain controller was expected.

(U//~~FOUO~~) [redacted] b7E

[redacted]

(U//~~FOUO~~) For more detailed information related to failed login attempts to the Exchange server and domain controller, see [redacted]-CYBER, serials 24 and 28. b3 b7E

(U//~~FOUO~~) [redacted] IP ADDRESS ANALYSIS (2015)

(U) (S//~~NF~~) Investigative activity conducted under MIDYEAR EXAM revealed [redacted] IP addresses used by [redacted], an administrator of the PRN Server, to log in to [redacted] under his control between March and August 2015 [redacted] The IP address was [redacted] b6 b7C b7E

[redacted] b1 b3 b6 b7C b7E

[k] (U//~~FOUO~~) [redacted] used the IP address to log in remotely to the PRN Server to administer the network and e-mail server.

b1
b3
b7E

~~SECRET//ORCON/NOFORN~~ [redacted] (X)

FEDERAL BUREAU OF INVESTIGATION

[redacted] (X)

b1
b3
b6
b7C
b7E

(X)//~~FOUO~~) Full details about the suspicious activity concerning [redacted] IP address [redacted] can be found in [redacted] CYBER, serial 20. (X)

◆◆